NACHRICHTEN AG

13. Juli 2025

Bundesregierung in Cybersicherheit-Chaos: Alarmstufe Rot!

Cyberangriffe auf Sachsen-Anhalt: IT-Sicherheit der Bundesregierung kritisch. Mangelnde Standards und zentrale Konzepte gefordert.

Sachsen-Anhalt, Deutschland - In dieser Woche haben gleich mehrere besorgniserregende Vorfälle die Cybersicherheit in Deutschland in den Fokus gerückt. Nachdem die Websites der Landesregierung Sachsen-Anhalt lahmgelegt wurden, gab es zudem einen Hackerangriff auf den Krankenhauskonzern Ameos. Diese Angriffe werfen ein grelles Licht auf die Sicherheitslage der IT-Systeme der Bundesregierung und ihrer Behörden, die laut einem aktuellen Bericht des Bundesrechnungshofes alles andere als sicher sind. So erfüllen lediglich 10 % der Rechenzentren des Bundes den notwendigen Mindeststandard für IT-Sicherheit, wie MDR berichtet.

Der Bericht thematisiert die gravierenden Mängel bei der IT-

Sicherheit in der Bundesverwaltung. So fehlt es an einer adäquaten Notstromversorgung, und es gibt keine Tests darüber, ob die Backups im Notfall funktionieren. Das Ergebnis dieser Missstände wird als ȝverheerendȝ bezeichnet. Angesichts der vielen Akteure im Bereich Cybersicherheit, insgesamt 370, herrscht ein regelrechter ȝDschungelȝ an Zuständigen, was die Koordination und Effektivität der Maßnahmen erschwert.

Einheitliches Konzept gefordert

Eine klare Aufgabenverteilung zwischen dem Innen- und dem Digitalministerium soll bis August festgelegt werden, während Bundesinnenminister Alexander Dobrindt ein Zentrum für Cyberabwehr vorgeschlagen hat. Experten drücken ihre Besorgnis über die fehlende zentrale Steuerung und die lückenhafte Kommunikation über Cyber-Vorfälle aus. ȝEs ist unerlässlich, dass wir hier endlich verbindliche Standards setzenȝ, so ein Fachmann im Interview mit Spiegel.

Im Kontext der allgemeinen Cybersicherheit in Deutschland spricht der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) von weiteren alarmierenden Trends. Die professionelle Arbeitsweise von Cyberkriminellen und der Anstieg von Ransomware-Angriffen kennen keine Grenzen. Im ersten Halbjahr 2024 kam es zu einem signifikanten Anstieg hochvolumiger DDoS-Angriffe, wobei gerade kleine und mittlere Unternehmen sowie Kommunen besonders betroffen sind. Ein krasser Vorfall im Oktober 2023, der 72 Kommunen und 20.000 Arbeitsplätze tangierte, zeigt, wie ernst die Lage tatsächlich ist, so BSI.

Zusammenarbeit als Schlüssel zur Sicherheit

In Anbetracht dieser Entwicklungen empfiehlt sich eine verstärkte Zusammenarbeit aller Beteiligten: Hersteller, Betreiber und Verbraucher müssen gemeinsam an der Resilienz

gegen Cyberkriminalität arbeiten. Die digitale Transformation Deutschlands vergrößert die Angriffsfläche stetig, und die Zahl der täglich bekannt werdenden Schwachstellen nimmt zu. Kritische Schwachstellen, insbesondere in Perimetersystemen wie Firewalls und VPNs, erfordern dringliche Aufmerksamkeit.

Die Maßnahmen des BSI zur frühzeitigen Erkennung und Warnung vor Bedrohungen sind ein Schritt in die richtige Richtung. Doch ohne die Einführung einer umfassenden und strukturierten Cyberabwehr bleibt die Bundesverwaltung verwundbar. Es ist an der Zeit, dass die Verantwortlichen auch handeln, denn die Cyberwelt schläft nicht.

Details	
Ort	Sachsen-Anhalt, Deutschland
Quellen	• www.mdr.de • www.spiegel.de • www.bsi.bund.de